

## UNITED STATES DISTRICT COURT

for the

Central District of California

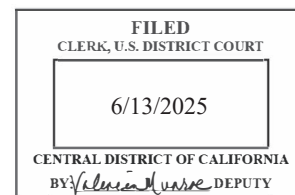
United States of America,

v.

EDWIN OSVALDO MANRIQUEZ,

Defendant.

Case No. 2:25-MJ-03653-DUTY



**CRIMINAL COMPLAINT BY TELEPHONE  
OR OTHER RELIABLE ELECTRONIC MEANS**

I, Ramel Moore, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date of June 9, 2025, in the county of Los Angeles in the Central District of California, the defendant violated:

*Code Section*

18 U.S.C. § 111

*Offense Description*

Assault on a Federal Officer

This criminal complaint is based on these facts:

*Please see attached affidavit.*☒ Continued on the attached sheet.

/s/

*Complainant's signature*

Ramel Moore, Special Agent

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone. ✎

Date: 6/13/25

A handwritten signature in black ink, appearing to read "Charles F. Eick".

*Judge's signature*

City and state: Los Angeles, California

Hon. Charles F. Eick, U.S. Magistrate Judge

*Printed name and title*

**AFFIDAVIT**

I, Ramel Moore, being duly sworn, declare and state as follows:

**I. PURPOSE OF AFFIDAVIT**

1. This affidavit is made in support of a criminal complaint and arrest warrant against Edwin Osvaldo MANRIQUEZ ("MANRIQUEZ") for a violation of 18 U.S.C. § 111 (Assault on a Federal Officer).

2. This affidavit is made in support of an application for a warrant to search the following digital device:

a. A grey Apple iPhone seized from Edwin Osvaldo MANRIQUEZ's person on June 13, 2025 ("SUBJECT DEVICE"), in the custody of the Federal Bureau of Investigation ("FBI"), in Los Angeles, California, and as further described in Attachment A.

3. The requested search warrant seeks authorization to seize evidence, fruits, and instrumentalities of a violation of 18 U.S.C. § 111 (Assault on Federal Officer) (the "Subject Offense").

4. Attachments A and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all

conversations and statements described in this affidavit are related in substance and in part only, all amounts or sums are approximate, and all dates and times are on or about those indicated.

## **II. BACKGROUND OF SPECIAL AGENT**

6. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since December 2021. Upon joining the FBI, I attended and graduated from the FBI Basic Special Agent Training Course in Quantico, Virginia where I received training in a variety of investigative and legal matters, including case management, interviewing and interrogation, crisis management, crime scene analysis, cellular telephone analysis, evidence collection, social media exploitation, and handling confidential sources. From April 2022 to July 2023, I was assigned to the Los Angeles Metropolitan Task Force on Violent Gangs ("LAMTFVG"), where I investigated gang activity and criminal enterprises.

7. I am currently assigned to the FBI Los Angeles Field Division's Violent Crime Task Force ("VCTF"), which is comprised of law enforcement officers from the FBI, Los Angeles Police Department ("LAPD"), and other federal, state, and local law enforcement agencies. As a member of the VCTF, I am responsible for investigating kidnappings, murders, robberies, extortion, and other violent crimes. My investigations have included the use of investigative techniques to include surveillance; execution of search, seizure, and arrest warrants; telephone

toll records; pen registers and trap traces; among other investigative techniques.

8. I have received basic training on cellular survey analysis and geo-location from the FBI Cellular Analysis and Survey Team ("CAST"). The training entailed utilizing cellular tower logs to identify subject phones from different crimes, even when it was not clear whether a cell phone was in use during the commission of the crime. I have also analyzed tower dump data sets and historical cell site data sets in my own investigations.

#### **IV. STATEMENT OF PROBABLE CAUSE**

9. Based on my review of law enforcement reports, social media videos, conversations with other law enforcement agents, witnesses, and the victim, and my own knowledge of the investigation, I am aware of the following:

##### **A. Paintballs are Shot at Federal Officers**

10. On June 9, 2025, protestors gathered in front of the federal building at 300 North Los Angeles Street in Los Angeles. During the protest, there was a street fight amongst the protestors where no law enforcement was involved. Federal Protective Service ("FPS") officers walked to the Temple Street side of the building to provide coverage so that protestors did not walk up the ramp to enter the federal building.

11. Once the fight dispersed, FPS officers walked back to the main entrance. At approximately 4:00 p.m., a white 2005 Infiniti G35 coupe, bearing California license plate number 8SGF019 ("Subject Vehicle"), stopped in the middle of the

street. The victim FPS officer ("E.S.") immediately noticed a paintball gun extended out of the passenger window of the Subject Vehicle. Initially, it appeared the suspect pulled the trigger, but nothing dispersed.

12. The suspect, who was in the passenger seat, and the driver suspect, continued to drive north on Los Angeles Street. The passenger suspect pulled the trigger multiple times and multiple rounds of paintballs were dispersed. The passenger suspect was wearing a light-grey and long-sleeve hoodie with a dark head covering, and the driver suspect was wearing a light and black face covering and a dark head covering.



13. E.S. was hit. The paintballs hit him on the head, left ear, left cheek, left neck, and left shoulder. E.S. was wearing a helmet and protective gear.

14. The passenger suspect then threw a hand sign with his left hand while still holding the paintball gun in his right hand. The Subject Vehicle then completed a U-turn, drove down Los Angeles Street, turned right on Temple Street, and then was out of view of the FPS officers.

**B. Identification of Subject Vehicle and Residence**

15. A video captured the license plate of the Subject Vehicle. FBI ran the license plate in law enforcement databases and confirmed that the car was registered to an individual named D.D. FBI further obtained D.D.'s identifiers, including date of birth, last known address, and telephone number.

16. The telephone number, ending in -9029 (the "Subject Telephone"), was registered to D.D. FBI submitted an emergency disclosure request to Verizon and received cell-site location records. The FBI did an analysis of those records and found that the Subject Telephone, which belonged to D.D., was in the vicinity of the federal building on 300 North Los Angeles Street at approximately 4:00 p.m.

17. The FBI also found through a public records check and DMV records that D.D. resided at the Subject Premises. The FBI conducted surveillance on the Subject Premises, and they saw the Subject Vehicle parked in the driveway of the Subject Premises.

**C. Federal Search Warrants Executed and Arrest of MANRIQUEZ**

18. On June 11, 2025, the Honorable Charles F. Eick, U.S. Magistrate Judge for the Central District of California, issued federal search warrants for the Subject Residence (case no. 2:25-MJ-3581), Subject Vehicle (case no. 2:25-MJ-3584), and D.D.'s persons (case no. 2:25-MJ-3585). The FBI executed these warrants on June 13, 2025.

19. FBI agents found the paintball gun used in the assault in D.D.'s garage and paintballs in the Subject Vehicle and in the garage near the paintball gun.

20. Further, FBI Mirandized D.D., and D.D. waived his Miranda rights and agreed to speak. D.D. admitted to being the driver of the Subject Vehicle during the time of the assault. D.D. also admitted that the paintball gun found was the gun used during the assault. He said he was the driver of the Subject Vehicle at the time of the assault, MANRIQUEZ was the shooter, and another individual was in the back seat. They were all wearing face coverings.

21. D.D. disagreed with MANRIQUEZ shooting at federal officers. In text messages between D.D. and MANRIQUEZ, the following was exchanged on the night of June 9, 2025, the same day the shooting occurred:

- D.D.: "Nigga they tryna get anybody who did shit I'm looking at the news and if they come for me for that paintball cuhhh I'm sorry bruh but I ain't going to jail"
- MANRIQUEZ: "nigga they ain't honna get us"
- MANRIQUEZ: "we had our face covered"
- D.D.: "I told u not to shoot them bruh they not part of immigration it was only for ice not cops"
- D.D.: "That don't matter"
- D.D.: "I had my car there"
- D.D.: "Plates out"
- MANRIQUEZ: "they ain't trust"
- D.D.: "If they do nigga I'm sorry"

- D.D.: "Bc they already tryna get that nigga who threw rocks at the cop cars that went viral"
- D.D.: "Bc his rock went through and hit the driver so they looking for him for assault"
- D.D.: "And u literally shot one in the face bro frl frl better hope they don't come to me"
- MANRIQUEZ: "they not gonna do anything"
- . . .
- MANRIQUEZ: "thats why i had ts tucked in and didnt take it out the shit"
- MANRIQUEZ: "that wouldn't prove shit"
- MANRIQUEZ: "they"
- D.D.: "Hmmm we'll see then cuz plates were out"
- MANRIQUEZ: "they ain't gonna prove it"
- MANRIQUEZ: "cause it wasn't showing outside"

22. D.D. positively identified MANRIQUEZ's CalDMV photograph as well as the address. FBI subsequently arrested MANRIQUEZ approximately 10 minutes from MANRIQUEZ's residence, and the FBI also seized the SUBJECT DEVICE from MANRIQUEZ's person.

#### **V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES**

23. As used herein, the term "digital device" includes the SUBJECT DEVICE.

24. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and

who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

25. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

26. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that

appears to have a biometric sensor and falls within the scope of the warrant: (1) depress MANRIQUEZ's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of MANRIQUEZ's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

**VI. CONCLUSION**

27. For all of the reasons described above, there is probable cause to believe that MANRIQUEZ has committed a violation of the Subject Offense, and there is probable cause to believe that evidence, fruits, instrumentalities of the Subject Offense will be found in the SUBJECT DEVICE.

Attested to by the applicant  
in accordance with the  
requirements of Fed. R. Crim.  
P. 4.1 by telephone on this  
13th day of June 2025.

A handwritten signature in black ink, appearing to read 'C. F. Eick', written over a horizontal line.

HON. CHARLES F. EICK  
UNITED STATES MAGISTRATE JUDGE